

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 753 860

(21) N° d'enregistrement national : 96 11915

(51) Int Cl⁶ : H 04 L 9/32, H 04 M 3/50

(12) DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 25.09.96.

(30) Priorité :

(43) Date de la mise à disposition du public de la
demande : 27.03.98 Bulletin 98/13.

(56) Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule.*

(60) Références à d'autres documents nationaux
apparentés :

(71) Demandeur(s) : FINTEL SOCIETE ANONYME — FR.

(72) Inventeur(s) : ROSSET FRANK, GAYET ALAIN et
MOULIN JEAN.

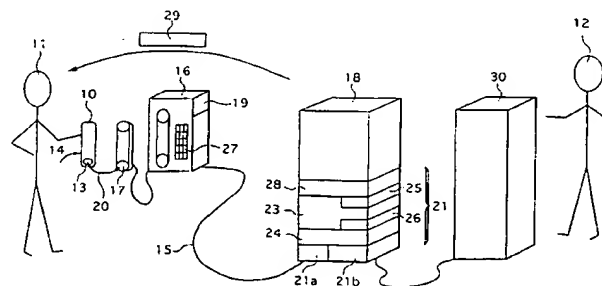
(73) Titulaire(s) :

(74) Mandataire : CABINET PATRICE VIDON.

(54) PROCÉDE ET SYSTÈME POUR SECURISER LES PRESTATIONS DE SERVICES A DISTANCE DES
ORGANISMES FINANCIERS.

(57) L'invention concerne un procédé et un système permettant aux clients (11) d'une banque ou d'une compagnie d'assurance (12), située à distance, d'accéder de manière sûre et rapide, au moyen d'un microphone (17) relié à un réseau de communication (15), aux services (30) offerts par cette banque ou cette compagnie d'assurance (12). Le procédé comprend les étapes suivantes:

- la banque ou la compagnie d'assurance (12) met à la disposition de chacun de ses clients (10) une carte (10) personnalisée, au format carte de crédit,
- ladite carte (10) émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par le client (11),
- lesdits signaux acoustiques sont reçus par le microphone (17) et transmis par le réseau de communication (15) au service informatique (18) de la banque ou de la compagnie d'assurance (12),
- les signaux d'identification sont traités et décryptés (24) électroniquement par le service informatique (18) de la banque ou de la compagnie d'assurance et les données obtenues après traitement et décryptage sont comparées (25) aux données d'identification de la carte et du client détenues (23) par le service informatique (18) de la banque ou de la compagnie d'assurance.



FR 2 753 860 - A1



Procédé et système pour sécuriser les prestations de services à distance des organismes financiers.

Le domaine de l'invention est celui des prestations de services à distance proposées par les organismes financiers, tels que les banques et/ou les compagnies d'assurances, à leur clients.

Plus précisément l'invention concerne un procédé et un système permettant aux clients d'une banque ou d'une compagnie d'assurance, située à distance, d'accéder de manière sûre et rapide, au moyen d'un microphone relié à un réseau de communication, aux services que la dite banque ou la dite compagnie d'assurance offre à ses clients.

Le problème posé est d'empêcher un utilisateur mal intentionné d'accéder aux services offerts par la banque ou la compagnie d'assurance sans y être autorisé, sans acquitter les droits correspondants ou en prétendant qu'il n'a pas demandé les services qui lui sont débités.

Pour résoudre ce problème il a été proposé d'utiliser des clés d'accès que le client génère au moyen d'équipement périphériques. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un autre problème : concevoir un procédé et un système commode d'utilisation, rapide à mettre en oeuvre en oeuvre et économique. En effet, dès lors que l'on s'adresse à un large public, la facilité d'utilisation et les gains de temps deviennent des problèmes majeurs qui ne peuvent pas être écartés. Ces objectifs sont atteints et ces problèmes sont résolus selon l'invention à l'aide d'un procédé comprenant les étapes suivantes :

- la banque ou la compagnie d'assurance met à la disposition de chacun de ses clients une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque client,
- la dite carte émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par le client de la banque ou de la compagnie d'assurance,
- lesdits signaux acoustiques sont reçus par le microphone et transmis par le réseau de communication au service informatique de la banque ou de la compagnie d'assurance,

- les signaux d'identification sont traités et décryptés électroniquement par le service informatique de la banque ou de la compagnie d'assurance et les données obtenues après traitement et décryptage sont comparées aux données d'identifications de la carte et du client détenus par le service informatique de la banque ou de la compagnie d'assurance.

5 Ainsi, grâce à ce procédé, la banque ou la compagnie d'assurance, peuvent vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Par ailleurs elles ont pu identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'elles offrent. De sorte qu'en cas de conformité le client est immédiatement mis en communication avec le serveur vocal de la banque ou de la

10 compagnie d'assurance.

 Afin d'augmenter la sécurité du procédé, dans une variante de réalisation, le procédé comprend en outre l'étape suivante : le client émet, au moyen d'un clavier associé au microphone et/ou à la carte, un code confidentiel ; après transmission au service informatique de la banque ou de la compagnie d'assurance, par le réseau de

15 communication, ce code confidentiel est traité et comparé au code confidentiel personnel du client détenu par le service informatique de la banque ou de la compagnie d'assurance.

 Ainsi, la banque ou la compagnie d'assurance peuvent vérifier que l'appelant est bien la personne habilitée à entrer en relation avec leurs services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

20 Avantageusement les signaux acoustiques émis par la carte varient à chaque opération.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du procédé et d'éviter que le client ne puisse pas contester l'ordre qu'il a passé à la banque ou à la compagnie d'assurance, le procédé comprend en outre les étapes suivantes :

- 25 - les ordres donnés par le client à la banque ou à la compagnie d'assurance sont validés par le client en actionnant la carte pour qu'elle émette un signal acoustique crypté de validation,
- ledit signal de validation est enregistré par le service informatique.

 Avantageusement un accusé de réception est adressé au client.

30 Grâce à ce procédé, le client a validé, par une signature électronique, l'ordre qu'il a donné

à la banque ou à la compagnie d'assurance.

L'invention concerne également un système permettant aux clients d'une banque ou d'une compagnie d'assurance, située à distance, d'accéder de manière sûre et rapide, aux services que la dite banque ou la dite compagnie d'assurance offre à ses clients. Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

Plus particulièrement, le système selon l'invention comprend :

- une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque client, mise à la disposition de celui-ci par la banque ou la compagnie d'assurance. La carte comporte des moyens d'émission de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie. Ces signaux acoustiques sont émis lorsque le client actionne les moyens d'émission au moyen d'un élément accessible de l'extérieur de la carte.

- des moyens de transformation des signaux acoustiques, notamment un combiné téléphonique comportant un microphone, en des signaux électroniques transmissibles à distance au moyen d'un réseau de communication.

- des moyens informatiques, dépendants des services informatiques de la banque ou de la compagnie d'assurance, connectés au réseau de communication et situés à distance des moyens d'émission des signaux acoustiques. Ces moyens informatiques comprennent eux-mêmes :

* une base de données contenant les références des cartes et des clients et leurs données d'identification,

* des moyens de traitement et de décryptage des signaux électroniques permettant d'obtenir des données caractéristiques des clients et des cartes,

* des moyens de comparaison des données d'identification contenues dans la base de données et des données caractéristiques des clients et des cartes.

De sorte qu'en cas de conformité, les services de la banque ou de la compagnie d'assurance sont immédiatement accessibles aux clients.

Afin d'augmenter la sécurité du système, dans une variante de réalisation, le système comprend en outre des seconds moyens de comparaison d'un code confidentiel

personnel au client contenu dans la base de données, à un code confidentiel émis par le client. Ce code est émis au moyen d'un clavier associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de la banque ou de la compagnie d'assurance, par le réseau de communication.

5 Ainsi, la banque ou la compagnie d'assurance peuvent vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

10 Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a passé à la banque ou à la compagnie, le système est tel que :

- la carte émet, lorsqu'elle est actionnée par le client, un signal acoustique crypté de validation des ordres donnés par le client,
- les moyens informatiques comprennent des moyens de détection et d'enregistrement du signal de validation.

15 Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à la banque ou à la compagnie d'assurance.

 Avantageusement les moyens informatiques comprennent des moyens d'édition d'un accusé de réception des ordres donnés, destiné à être adressé au client.

20 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description d'une variante de réalisation de l'invention, donnée à titre d'exemple indicatif et non limitatif, et de la figure 1 annexée présentant une vue schématique en perspective du système et du procédé selon l'invention.

25 Le système et le procédé selon l'invention permettent au client 11 disposant d'un combiné téléphonique 16 comportant un microphone 17, d'accéder de manière sûre et rapide, aux services 30 que la banque ou la compagnie d'assurance 12 offrent à leurs clients 11. Le combiné téléphonique 16, situé à distance des services informatiques 18 du prestataire de services 12, est connecté aux services informatiques via un réseau de communication 15.

30 Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque client 11. Cette carte est

mise à la disposition des leurs clients par la banque ou la compagnie d'assurance 12 . La carte 10 comporte des moyens d'émission de brefs signaux acoustiques d'identification 13, de type DTMF, cryptés au moins en partie. Ces signaux sont émis lorsque les moyens d'émission 13 sont actionnés par l'utilisateur au moyen d'un élément 14 accessible de l'extérieur de la carte (non visible sur la figure car situé sur l'autre côté de la carte). Les signaux acoustiques 20 sont reçus par le microphone 17 du combine téléphonique, contre lequel l'utilisateur accole la carte 10. Le système comprend également des moyens 19 de transmission des signaux acoustiques 20, situés dans le combiné téléphonique 16. Ces moyens de transmission transmettent à distance les signaux, après traitement, via le réseau de communication 15. Le système comprend également des moyens informatiques 21, dépendant des services informatiques 18 de la banque ou de la compagnie d'assurance. Ces moyens informatiques sont connectés au réseau de communication 15 et situés à distance des combinés téléphoniques 16.

Ces moyens informatiques 21 comprennent eux-mêmes :

- * une base de données 23 contenant les références des cartes et des clients et leurs données d'identification,

- * des moyens de traitement et de décryptage 24 des signaux électroniques permettant d'obtenir des données caractéristiques des clients et des cartes,

- * des moyens de comparaison 25 des données d'identification contenues dans la base de données 23 et des données caractéristiques des clients et des cartes.

De sorte qu'en cas de conformité, les services 30 de la banque ou de la compagnie d'assurance sont immédiatement accessibles aux clients 11.

De préférence les moyens de cryptage de la carte et de décryptage des services informatiques sont conçus de telle sorte que le signal acoustique varie à chaque opération (horloge, compteur d'opérations etc., ainsi qu'il est notamment décrit dans les brevets US N° : 4,998,279 et US N° : 4,298,098). Ainsi l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques de la banque ou de la compagnie d'assurance et bénéficier des services de celui-ci.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée

sur la figure 1, le système comprend en outre des seconds moyens de comparaison 26. Ces moyens de comparaison permettent de comparer un code confidentiel personnel au client contenu dans la base de données avec le code confidentiel émis par l'utilisateur. Ce code est émis au moyen d'un clavier 27 associé au combiné téléphonique 16 et/ou à la carte 10 et transmis aux moyens informatiques 21 du prestataire, par le réseau de communication 15.

Ainsi, le prestataire de services à l'assurance que l'appelant 11 est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a adressé à la banque ou à la compagnie d'assurance, le système selon l'invention est tel que :

- la carte 10 émet, lorsqu'elle est actionnée 14 par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné 11,
- lesdits moyens informatiques 21 comprennent des moyens de détection 21a et d'enregistrement 21b du signal de validation.

Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

Avantageusement dans ce cas les moyens informatiques 21 comprennent en outre des moyens d'édition 28 d'un accusé de réception 29 des ordres donnés. Cet accusé de réception est adressé à l'abonné 11.

REVENDICATIONS

1. Procédé permettant aux clients (11) d'une banque ou d'une compagnie d'assurance (12), située à distance, d'accéder de manière sûre et rapide, au moyen d'un microphone (17) relié à un réseau de communication (15), aux services (30) que la dite banque ou la dite compagnie d'assurance (12) offre à ses clients (11),

caractérisé en ce qu'il comprend les étapes suivantes :

- la banque ou la compagnie d'assurance (12) met à la disposition de chacun de ses clients (10) une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque client,

- la dite carte (10) émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par le client (11) de la banque ou de la compagnie d'assurance (12),

- les dits signaux acoustiques sont reçus par le microphone (17) et transmis par le réseau de communication (15) au service informatique (18) de la banque ou de la compagnie d'assurance (12),

- les signaux d'identification sont traités et décryptés (24) électroniquement par le service informatique (18) de la banque ou de la compagnie d'assurance et les données obtenues après traitement et décryptage sont comparées (25) aux données d'identification de la carte et du client détenues (23) par le service informatique (18) de la banque ou de la compagnie d'assurance.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre l'étape suivante :

- le client émet, au moyen d'un clavier (27) associé au microphone (17) et/ou à la carte (20), un code confidentiel ; après transmission au service informatique (18) de la banque ou de la compagnie d'assurance, par le réseau de communication (15), ce code confidentiel est traité et comparé (26) au code confidentiel personnel du client détenu par le service informatique de la banque ou de la compagnie d'assurance.

3. Procédé selon les revendications 1 ou 2, caractérisé en ce qu'il comprend en outre l'étape suivante :

- les ordres donnés par le client à la banque ou à la compagnie d'assurance sont

validés par le client en actionnant (14) la carte (10) pour qu'elle émette un signal acoustique crypté de validation,

- ledit signal de validation est enregistré (21b) par le service informatique (18) de l'opérateur de la banque ou de la compagnie d'assurance.

5 4 . Procédé selon la revendication 3, caractérisé en ce qu'il comprend en outre l'étape suivante :

- un accusé de réception (29) du signal de validation est adressé au client (10) par la banque ou la compagnie d'assurance.

10 5 . Procédé selon l'une des revendications 1 à 4 caractérisé en ce que les signaux acoustiques émis par la carte varient à chaque opération.

6 . Système permettant aux clients (11) d'une banque ou d'une compagnie d'assurance (12), située à distance, d'accéder de manière sûre et rapide, aux services (30) que la dite banque ou la dite compagnie d'assurance offre à ses clients,

caractérisé en ce qu'il comprend :

15 - une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque client, mise à la disposition de ceux-ci ; la dite carte comportant des moyens (13) d'émission de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsque les dits moyens d'émission sont actionnés par le client de la banque ou de la compagnie d'assurance au
20 moyen d'un élément accessible (14) de l'extérieur de la carte,

- des moyens (17) de transformation des signaux acoustiques, notamment un combiné téléphonique comportant un microphone, en des signaux électroniques transmissibles à distance au moyen d'un réseau de communication (15),

25 - des moyens informatiques (21) , dépendants des services informatiques (18) de la banque ou de la compagnie d'assurance, connectés au réseau de communication (15) et situés à distance des moyens (17) d'émission des signaux acoustiques, les dits moyens informatiques comprenant :

* une base de données (23) contenant les références des cartes et des clients et leurs données d'identification,

30 * des moyens de traitement et de décryptage (24) des signaux électroniques

permettant d'obtenir des données caractéristiques des clients et des cartes,

* des moyens de comparaison (25) des données d'identification contenues dans la base de données et des données caractéristiques des clients et des cartes,

de sorte qu'en cas de conformité, les services de la banque ou de la compagnie d'assurance sont immédiatement accessibles aux clients.

7. Système selon la revendication 6, caractérisé en ce que lesdits moyens informatiques comprennent en outre:

- des seconds moyens de comparaison (26) d'un code confidentiel personnel au client contenu dans la base de données, à un code confidentiel émis par le client au moyen d'un clavier associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de la banque ou de la compagnie d'assurance, par le réseau de communication (15).

8. Système selon les revendications 6 ou 7, caractérisé en ce que :

ladite carte (10) émettant en outre, lorsqu'elle est actionnée (14) par le client, un signal acoustique crypté de validation des ordres donnés par le client,

et en ce que lesdits moyens informatiques comprennent en outre :

- des moyens de détection (21a) et d'enregistrement (21b) du signal de validation.

9. Système selon la revendication 8, caractérisé en ce que lesdits moyens informatiques comprennent en outre :

- des moyens d'édition (28) d'un accusé de réception (29) des ordres donnés, destiné à être adressé au client.

10. Système selon l'une des revendications 6 à 9, caractérisé en ce que la carte comporte des moyens de cryptage permettant de varier les signaux acoustiques d'une opération à l'autre.

1/1

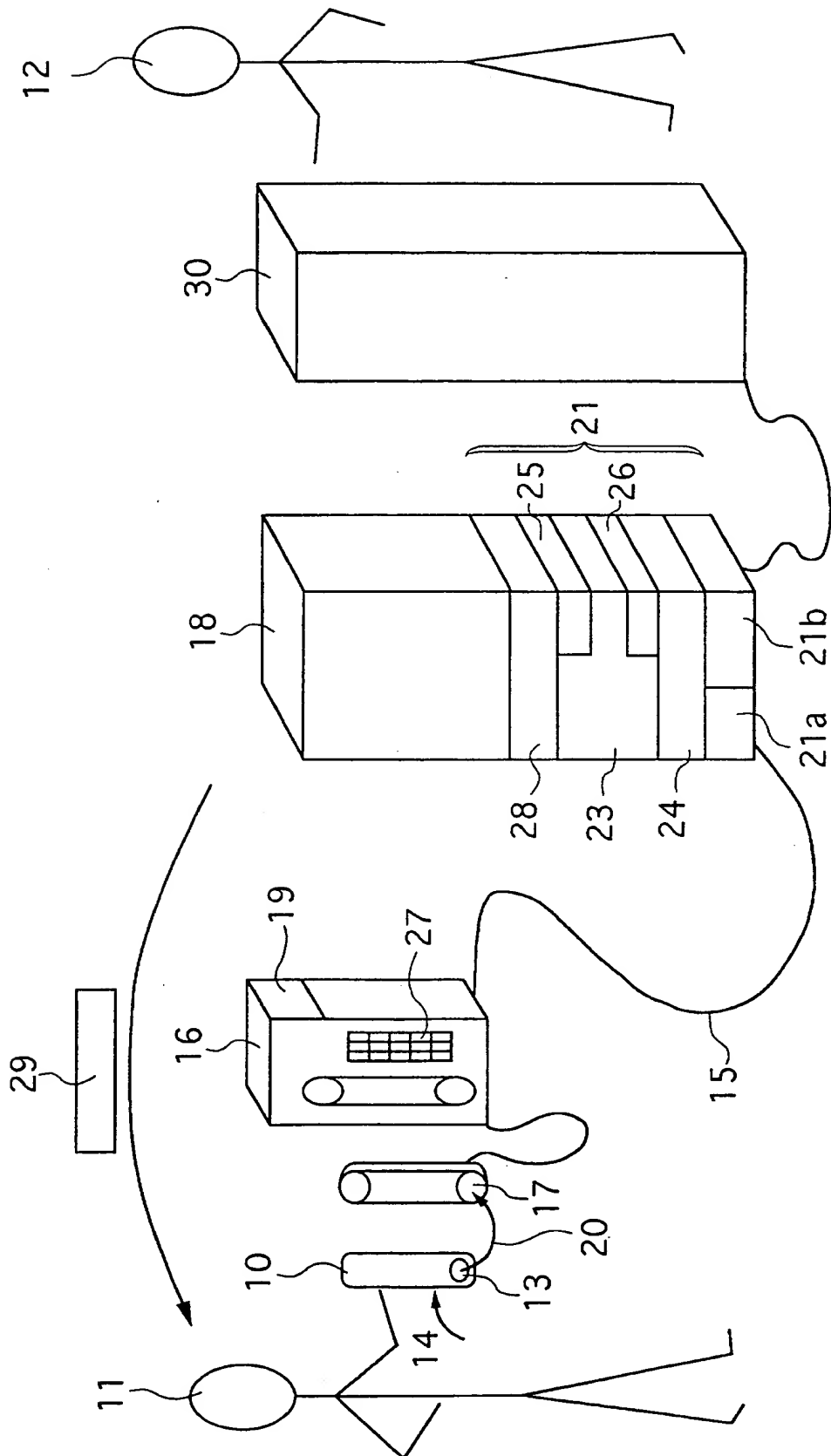


Fig. 1

INSTITUT NATIONAL

de la

PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE
PRELIMINAIREétabli sur la base des dernières revendications
déposées avant le commencement de la rechercheFA 533651
FR 9611915

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	CA 2 085 775 A (BOURRE MICHEL ; LAZZARINI GABRIEL (CA); TROLI JOHN (CA)) 19 Juin 1994 * le document en entier *	1,6
Y	FR 2 701 181 A (GORETA) * page 1, ligne 1 - ligne 29 *	1,6
A	GB 2 274 523 A (PATNI CHANDRA KAMAR) 27 Juillet 1994 * page 2, alinéa 4 *	4,5,9,10
A	DE 43 25 459 A (EISELE) * colonne 2, ligne 64 - colonne 3, ligne 15 * * colonne 3, ligne 62 - colonne 4, ligne 55 * * colonne 3, ligne 62 - colonne 4, ligne 55 *	1-3,6-8
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		H04L H04M
Date d'achèvement de la recherche		Examineur
16 Juin 1997		Holper, G.
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>		